Comment. Math.
Univ. St. Pauli
XXIII—2, 1974

On the coefficients of the cyclotomic polynomials

by

Mikihiko ENDO

(Received November, 7, 1974)

1. The cyclotomic polynomial $F_n(x)$ is defined as the polynomial whose roots are the primitive n-th roots of unity. Let $m=\varphi(n)$ (Euler function), then the polynomial is of the form

$$F_n(x)=\prod_{\omega}{}'(x-\omega)=x^m+c_1x^{m-1}+\cdots+c_{m-1}x+c_m\ .$$

Here, we use the symbol $\prod_{\omega}{}'$ to mean the product in which ω runs over all the primitive n-th roots of unity. It is well known that the coefficients c_k are rational integers and $c_{m-k}=c_k$ for all $k=1, 2, \cdots, m-1$. It is also known that if $n<105$, all the coefficients c_k are ±1 or 0 (Erdös [2]). For $n=105$, the coefficient -2 occurs for the first time, in fact, $c_7=-2$ in this case. We shall show in this paper that $k=7$ is the minimal number for which $|c_k|>1$ (for some n). For this purpose, we give an expression of c_k using Möbius functions and binomial coefficients [Theorem]. And as an application of the formula, we give our result.

2. Möbius function $\mu(n)$ is usually defined for the natural number n. But, for our later use, we define it for non-integral rational numbers n/d, setting $\mu(n/d)=0$. Then, we have

LEMMA 1.

$$\sum_{\omega}{}'\omega^s=\sum_{d|s}d\cdot\mu\left(\frac{n}{d}\right)\ .$$

Proof. By $\sum_{(d)}$ and $\sum_{(d)}{}'$, we shall mean the sums with respect to all the d-th roots and all the primitive d-th roots of the unity, respectively. Therefore, $\sum_{(n)}{}'$ has the same meaning as $\sum_{\omega}{}'$. It is clear that

$$\sum_{(n)}\omega^s=\sum_{d|n}\left(\sum_{(d)}{}'\omega^s\right)\ .$$

Then, by the Möbius' reciprocity,

$$\sum_{(n)}{}'\omega^s=\sum_{d|n}\left(\sum_{(d)}\omega^s\right)\mu\left(\frac{n}{d}\right)=\sum_{d|n}\sum_{d|s}d\cdot\mu\left(\frac{n}{d}\right)\ ,$$

since $\sum_{(d)} \omega^s = d$ for $d \mid s$ and $=0$ otherwise. By our definition of Möbius function, $\mu(n/d)=0$ if $d \nmid n$, so that we can put the equation into

$$\sum_{(n)}{}' \omega^s = \sum_{d \mid s} d \cdot \mu\left(\frac{n}{d}\right). \qquad \text{q.e.d.}$$

We also use the binomial coefficients:

$$\binom{a}{k} = \frac{a(a-1)\cdots(a-k+1)}{k!}.$$

We shall define $\binom{a}{0}=1$ for all a and $\binom{0}{k}=0$ for $k \geqq 1$.

LEMMA 2. $$k\binom{a}{k} = a\sum_{d=1}^{k} (-1)^{d+1}\binom{a}{k-d}.$$

Proof. Since

$$k\binom{a}{k} = \frac{a(a-1)\cdots(a-k+2)(a-k+1)}{(k-1)!}$$
$$= a\frac{a(a-1)\cdots(a-k+2)}{(k-1)!} - (k-1)\frac{a(a-1)\cdots(a-k+2)}{(k-1)!},$$

our Lemma is proved by induction. q.e.d.

3. By the relation of the roots and the coefficients, we know that

$$(-1)^k \cdot c_k = \sum_{\omega_1,\cdots,\omega_k}{}' \omega_1 \cdot \omega_2 \cdots \omega_k, \qquad \cdots(1)$$

where $\{\omega_1, \cdots, \omega_k\}$ runs over all the k-combinations of the primitive n-th roots of unity. An elementary calculation shows that

$$k \sum_{\omega_1,\cdots,\omega_k}{}' \omega_1\omega_2\cdots\omega_k = \sum_{s=1}^{k} (-1)^{s+1}\left(\sum_{\omega_1,\cdots,\omega_{k-s}}{}' \omega_1 \cdot \omega_2 \cdots \omega_{k-s}\right)\left(\sum{}' \omega^s\right). \qquad \cdots(2)$$

Using these expressitions, we can now prove

THEOREM

$$c_k = \sum_{i_1+2i_2+\cdots+ki_k=k} (-1)^{i_1+\cdots+i_k}\binom{\mu(n)}{i_1}\binom{\mu(n/2)}{i_2}\cdots\binom{\mu(n/k)}{i_k},$$

where $\{i_1, i_2, \cdots, i_k\}$ *runs over all the non-negative integral solutions of the equation* $i_1+2i_2+\cdots+ki_k=k$.

Proof. We shall prove our Theorem by induction on k.

For $k=1$, $i_1=1$ is the only possible value for i_1, and the right hand side of the equation is

$$(-1)^{i_1}\cdot\binom{\mu(n)}{i_1}=-\binom{\mu(n)}{1}=-\mu(n)\ .$$

and this equal to $c_1=-\sum'\omega$ by Lemma 1 and (1).

Now, assuming the equation for all values smaller than k, we shall prove it for k. By (1) and (2),

$$c_k=\frac{(-1)^k}{k}\sum_{s=1}^{k}(-1)^{s+1}\Big(\sum'_{\omega_1,\cdots,\omega_{k-s}}\omega_1\cdots\omega_{k-s}\Big)\Big(\sum'_{\omega}\omega^s\Big)=\frac{-1}{k}\sum_{s=1}^{k}c_{k-s}\Big(\sum'_{\omega}\omega^s\Big)\ .$$

By the inductions hypothesis and Lemma 1, we get

$$c_k=\frac{-1}{k}\sum_{s=1}^{k}\sum_{i_1+2i_2+\cdots+ki_k=k-s}(-1)^{i_1+\cdots+i_k}\binom{\mu(n)}{i_1}\binom{\mu(n/2)}{i_2}\cdots$$
$$\cdots\binom{\mu(n/k)}{i_k}\cdot\sum_{d\mid s}d\cdot\mu\Big(\frac{n}{d}\Big)\ .$$

Note that the equation $i_1+2i_2+\cdots+ki_k=k-s$ is equivalent to the equation $i_1+2i_2+\cdots+(k-s)\cdot i_{k-s}=k-s$, since we have assumed that $i_h\geqq 0$ for all $h=1, 2, \cdots, k$ and so $i_{k-s+1}=\cdots=i_k=0$. Therefore,

$$c_k=-\sum_{s=1}^{k}\sum_{d\mid s}\sum_{i_1+\cdots+k\cdot i_k=k-s}(-1)^{i_1+\cdots+i_k}\frac{d}{k}\binom{\mu(n)}{i_1}\cdots$$
$$\cdots\binom{\mu(n/(d-1))}{i_{d-1}}\cdot\mu\Big(\frac{n}{d}\Big)\binom{\mu(n/d)}{i_d}\cdots\binom{\mu(n/k)}{i_k}\ .$$

Setting $s/d=t$ and changing the order of summations, we get

$$c_k=-\sum_{d=1}^{k}\sum_{t=1}^{[k/d]}\sum_{i_1+\cdots+ki_k=k-dt}(-1)^{i_1+\cdots+i_k}\cdot\frac{d}{k}\binom{\mu(n)}{i_1}\cdots$$
$$\cdots\mu\Big(\frac{n}{d}\Big)\binom{\mu(n/d)}{i_d}\cdots\binom{\mu(n/k)}{i_k}\ .$$

Now, putting $i_d+t=j_d$ and $i_h=j_h$ for $h\neq d$, we get

$$c_k=\sum_{d=1}^{k}\sum_{j_1+2j_2+\cdots+k\cdot j_k=k}(-1)^{j_1+j_2+\cdots+j_k}\frac{d}{k}\cdot\binom{\mu(n)}{j_1}\cdots$$
$$\cdots\Big[\sum_{t=1}^{j_d}(-1)^{t+1}\mu\Big(\frac{n}{d}\Big)\binom{\mu(n/d)}{j_d-t}\Big]\cdots\binom{\mu(n/k)}{j_k}$$
$$=\sum_{j_1+\cdots+kj_k=k}(-1)^{j_1+\cdots+j_k}\sum_{d=1}^{k}\frac{d\cdot j_k}{k}\binom{\mu(n)}{j_1}\cdots\binom{\mu(n/d)}{j_d}\cdots\binom{\mu(n/k)}{j_k}$$

(by Lemma 2) .

Since $\sum_{d=1}^{k}d\cdot j_d=j_1+2\cdot j_2+\cdots+k\cdot j_k=k$, we have the requiring result:

$$c_k=\sum_{j_1+2j_2+\cdots+kj_k=k}(-1)^{j_1+j_2+\cdots+j_k}\binom{\mu(n)}{j_1}\binom{\mu(n/2)}{j_2}\cdots\binom{\mu(n/k)}{j_k}\ .\quad\text{q.e.d.}$$

Since the the number of the solutions of the equation $i_1+2i_2+\cdots+ki_k=k$ is equal to the pertition number $p(k)$ of k and since $\left|\binom{\mu(n/d)}{i_d}\right|\leqq 1$, we can get from Theorem a rough estimation of c_k, namely,

$$|c_k|\leqq p(k) \quad \text{(for any } n\text{)} .$$

But, for small k's, we can get more precise estimation.

4. The equation $i_1+2i_2=2$ has two solutions $(i_1, i_2)=(2, 0)$ and $(0, 1)$. Hence, by our Theorem,

$$c_2=\sum_{i_1+2i_2=2}(-1)^{i_1+i_2}\binom{\mu(n)}{i_1}\binom{\mu(n/2)}{i_2}=\binom{\mu(n)}{2}-\binom{\mu(n/2)}{1}$$
$$=\frac{1}{2}\mu(n)(\mu(n)-1)-\mu\left(\frac{n}{2}\right) .$$

If $\mu(n)=0$ or 1, $(1/2)\mu(n)(\mu(n)-1)=0$ so that $c_2=-\mu(n/2)$. If $\mu(n)=-1$, then $(1/2)\mu(n)(\mu(n)-1)=1$. In this case, if $n/2$ is an integer, then $\mu(n/2)=1$ and so $c_2=0$. And, if $n/2$ is not an integer, then $\mu(n/2)=0$ by our definition of $\mu(n)$, hence, we have $c_2=1$.

In any case, we have $|c_2|\leqq 1$.

In the same way, we can estimate the value of c_k for $k=3$, 4, 5, 6, and we get

$$|c_k|\leqq 1 \qquad (1\leqq k\leqq 6) .$$

Now, we shall estimate c_7.

I. When $\mu(n)=0$, then $\binom{\mu(n)}{i_1}=0$ for $i_1\geqq 1$. Therefore,

$$c_7=\sum_{2i_2+\cdots+7\cdot i_7=7}(-1)^{i_2+\cdots+i_7}\binom{\mu(n/2)}{i_2}\cdots\binom{\mu(n/7)}{i_7} .$$

The equation $2i_2+\cdots+7i_7=7$ has the four solutions $(i_2, \cdots, i_7)$:

$$i_2=2,\ i_3=1; \quad i_2=1,\ i_5=1; \quad i_3=1,\ i_4=1; \quad i_7=1 .$$

Hence,

$$c_7=-\frac{1}{2}\mu\left(\frac{n}{2}\right)\left(\mu\left(\frac{n}{2}\right)-1\right)\mu\left(\frac{n}{3}\right)+\mu\left(\frac{n}{2}\right)\mu\left(\frac{n}{5}\right)+\mu\left(\frac{n}{3}\right)\mu\left(\frac{n}{4}\right)-\mu\left(\frac{n}{7}\right) .$$

I-i) If $\mu(n/2)=1$, then n must be devisible by 4, and so $\mu(n/3)$, $\mu(n/5)$ and $\mu(n/7)$ must be 0. We have $c_7=0$.

I-ii) If $\mu(n/2)=0$ and $p^2\,|\,n$ with $p\neq 7$ or $7^3\,|\,n$, then

$$c_7=\mu\left(\frac{n}{3}\right)\mu\left(\frac{n}{4}\right)-\mu\left(\frac{n}{7}\right)=0 .$$

If $\mu(n/2)=0$ and $7^2\,||\,n$, then

$$c_7=-\mu\left(\frac{n}{7}\right).$$

I-iii) If $\mu(n/2)=-1$, then n must be divisible by 4 and so $\mu(n/3)=\mu(n/5)=\mu(n/7)$ nust be 0. Therefore we have $c_7=0$.

II. When $\mu(n)=1$, $\binom{\mu(n)}{i_1}=0$ for $i_1\geqq 2$ and so

$$c_7=\mu(n)\frac{1}{6}\mu\left(\frac{n}{2}\right)\left(\mu\left(\frac{n}{2}\right)-1\right)\left(\mu\left(\frac{n}{2}\right)-2\right)-\mu(n)\frac{1}{2}\mu\left(\frac{n}{3}\right)\left(\mu\left(\frac{n}{3}\right)-1\right)$$
$$+\mu(n)\mu\left(\frac{n}{6}\right)-\frac{1}{2}\mu\left(\frac{n}{2}\right)\left(\mu\left(\frac{n}{2}\right)-1\right)\mu\left(\frac{n}{3}\right)+\mu\left(\frac{n}{2}\right)\mu\left(\frac{n}{5}\right)-\mu\left(\frac{\mu}{7}\right),$$

since $\mu(n/4)=0$.

II-i) If n is not divisible by 2, then $\mu(n/2)=0$ and we have

$$c_7=-\frac{1}{2}\mu\left(\frac{n}{3}\right)\left(\mu\left(\frac{n}{3}\right)-1\right)-\mu\left(\frac{n}{7}\right)$$

Since $\mu(n)=1$, $\mu(n/7)=-1$ or 0, if $7\mid n$ or not, respectively. Therefore $-\mu(n/7)=1$ or 0. As the same way $-(1/2)\mu(n/3)(\mu(n/3)-1)=-1$ or 0, if $3\mid n$ or not, respectively. Therefore, we have also $|c_7|\leqq 1$.

II-ii) If n is divisible by 2, $\mu(n/2)=-1$ and so we have

$$c_7=-1-\frac{1}{2}\mu\left(\frac{n}{3}\right)\left(\mu\left(\frac{n}{3}\right)-1\right)+\mu\left(\frac{n}{6}\right)-\mu\left(\frac{n}{3}\right)-\mu\left(\frac{n}{5}\right)-\mu\left(\frac{n}{7}\right).$$

II-ii)-a) If n is not divisible by 3, then $\mu(n/3)=0$ so that

$$c_7=-1-\left(\mu\left(\frac{n}{5}\right)+\mu\left(\frac{n}{7}\right)\right).$$

But, $\mu(n/5)$ and $\mu(n/7)$ are 0 or -1, since $\mu(n)=1$. Hence, in this case, we have also

$$|c_7|\leqq 1.$$

II-ii)-b) If n is divisible by 3, then $\mu(n/3)=-1$ so that $\mu(n/6)=1$ and we have

$$c_7=-1-1+1+1-\mu\left(\frac{n}{5}\right)-\mu\left(\frac{n}{7}\right)=-\left\{\mu\left(\frac{n}{5}\right)+\mu\left(\frac{n}{7}\right)\right\}.$$

In this case, if $5\mid n$ and $7\mid n$, $c_7=2$. In fact, for $n=2\times 3\times 5\times 7=210$, we have $c_7=2$.

III. When $\mu(n)=-1$, $\binom{\mu(n)}{i_1}=(-1)^{i_1}$ and $\mu(n/4)=0$ since $n/4$ is not an integer.

Hence,

$$c_7=1-\mu\left(\frac{n}{2}\right)-\mu\left(\frac{n}{3}\right)+\frac{1}{2}\mu\left(\frac{n}{2}\right)\left(\mu\left(\frac{n}{2}\right)-1\right)+\mu\left(\frac{n}{2}\right)\mu\left(\frac{n}{3}\right)-\mu\left(\frac{n}{5}\right)$$
$$-\frac{1}{6}\mu\left(\frac{n}{2}\right)\left(\mu\left(\frac{n}{2}\right)-1\right)\left(\mu\left(\frac{n}{2}\right)-2\right)+\frac{1}{2}\mu\left(\frac{n}{3}\right)\left(\mu\left(\frac{n}{3}\right)-1\right)$$
$$-\mu\left(\frac{n}{6}\right)-\frac{1}{2}\mu\left(\frac{n}{2}\right)\left(\mu\left(\frac{n}{2}\right)-1\right)\mu\left(\frac{n}{3}\right)+\mu\left(\frac{n}{2}\right)\mu\left(\frac{n}{5}\right)-\mu\left(\frac{n}{7}\right).$$

Since $\mu(n)=-1$, $\mu(n/2)$ and $\mu(n/3)$ must be 1 or 0. Then,

$$c_7=\left(1-\mu\left(\frac{n}{2}\right)\right)\left(1-\mu\left(\frac{n}{3}\right)\right)-\mu\left(\frac{n}{5}\right)-\mu\left(\frac{n}{6}\right)+\mu\left(\frac{n}{2}\right)\mu\left(\frac{n}{5}\right)-\mu\left(\frac{n}{7}\right).$$

III-i) If $\mu(n/2)=1$,

$$c_7=-\mu\left(\frac{n}{6}\right)-\mu\left(\frac{n}{7}\right).$$

Since $\mu(n/2)=1$, $\mu(n/6)=0$ or -1. Also $\mu(n/7)=0$ or 1. We have

$$|c_7|\leqq 1.$$

III-ii) If $\mu(n/2)=0$, then $\mu(n/6)=0$ and

$$c_7=1-\mu\left(\frac{n}{3}\right)-\mu\left(\frac{n}{5}\right)-\mu\left(\frac{n}{7}\right).$$

Therefore, if $\mu(n/3)=\mu(n/5)=\mu(n/7)=1$, $c_7=-2$. In fact, for

$$n=3\times 5\times 7=105, \qquad c_7=-2.$$

As the conclusion, we have the followings:

Except in the cases i) $\mu(n)=1$ *and* n *is divisible by* $2\times 3\times 5\times 7$, *and* ii) $\mu(n)=-1$, $2\nmid n$ *but* n *is divisible by* $3\times 5\times 7$, *we have*

$$|c_7|\leqq 1.$$

In the case i), $c_7=-2$, *and in the case* ii) $c_7=2$.

Proffesor Iwata, H. (Toyama Univ.) informed me that $|c_8|$ and $|c_9|$ are also $\leqq 2$.

References

[1] BLOOM, D. M.; On the coefficients of the cyclotomic polynomials, Amer. Math. Monthly **75** (1968), 372-377.

[2] ERDÖS, P.; On the coefficients of the cyclotomic polynomial, Bull. of A.M.S. **52** (1946), 179-184.

Rikkyo University